EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

ENERGY AND COMMERCE COMMITTEE
RANKING MEMBER
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND
THE INTERNET

SELECT COMMITTEE ON
HOMELAND SECURITY

RESOURCES COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515–2107

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–2107
(202) 225–2836

DISTRICT OFFICES:
5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396–2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875–2900
www.house.gov/markey

February 23, 2004

The Honorable Tom Ridge
Secretary
Department of Homeland Security
Washington, DC 20528

The Honorable Donald H. Rumsfeld
Secretary
Department of Defense
Washington, DC 20301

The Honorable George Tenet
Director of Central Intelligence
Central Intelligence Agency
Washington, DC 20505

Dear Secretary Ridge, Secretary Rumsfeld and Director Tenet:

I am writing to express my concern about the potential damage to the nation's security that could result from the misuse of personal information that has been transmitted offshore by U.S.-based corporations.

Recent press reports suggest that many U.S. companies are transferring to offshore outsourcing firms for analysis or processing some of the most intimate personal data they have collected about American citizens, including individually-identifiable financial and medical information. A November 7, 2003 article in The San Francisco Examiner described the prevalence of this practice among credit agencies, reporting that "two of the three major credit-reporting agencies, each holding detailed files on about 220 million U.S. consumers, are in the process of outsourcing sensitive operations abroad, and a third may follow suit shortly."[1] In addition to the transfer overseas of customers' private data, corporations continue to move entire job functions abroad, particularly those that require regular access to confidential information, including payroll, benefits, accounting, and customer service functions. According to the director of Michigan State University's identity theft crime lab, increasingly easy availability of U.S. identities in potentially thousands of workplaces in foreign countries known for high crime rates can be expected to create a surge in identity theft in the years to come.[2]

For years, terrorists have used stolen or fraudulent identities and documents to enter the United States illegally. The National Commission on Terrorist Attacks Upon the United States

[1] "Credit Agencies Sending Our Files Abroad", San Francisco Examiner, November 7, 2003.
[2] "To Root Out Identity Theft, Set Restrictions in Workplace", Detroit Free Press, September 3, 2003.

("The 9-11 Commission") reported last month that passports belonging to two of the 9/11 hijackers "were manipulated in a fraudulent manner", while two other hijackers had passports with "suspicious indicators".[3] As personally identifiable information belonging to American citizens is increasingly sent abroad, the risk increases that terrorists could access, manipulate and misuse this information to infiltrate the United States.

To date, the Administration has not insisted that the personal information of U.S. citizens receive protection that is comparable to U.S. standards whenever the private data are exported. This failure to require comparable privacy safeguards leaves Americans exposed to serious risks of international identify theft or individual or institutional misuse of their confidential personal data by foreign companies or rogue employees of such companies. Additionally, because physical and electronic security standards for safeguarding confidential information may be considerably weaker outside of the U.S., this information may be more accessible to terrorists overseas who seek to use it to obtain documents for entering the United States.

In Pakistan, a country in which terrorists are known to operate actively, a Pakistani woman who had been hired by a Texas company to transcribe medical records for a California hospital threatened to post sensitive patient medical records on the Internet unless she received certain payments she claimed were due to her. The Pakistani woman reportedly posted one file on the Internet, demonstrating her willingness to carry out her threat if her demands were not met.[4]

This incident highlights the fact that, in their rush to cut costs and increase their bottom line, companies may be sacrificing the privacy protections the law affords to American citizens by transferring sensitive information to off-shore companies that are outside of the reach of U.S. privacy law and beyond the jurisdiction of U.S. regulators. Moreover, terrorists' long track record of using false identities and creating legitimate documents from stolen personal information raises concerns about the consequences to U.S. security that may result from the growing offshoring trend.

I therefore request that you respond to the following questions about the impact of offshoring on U.S. security and explain what steps are being undertaken by your department or agency to protect the privacy of personal information collected about American citizens by contractors or other persons subject to your oversight and supervision. Specifically, I request your assistance and cooperation in providing responses to the following questions:

1. Personally identifiable information such as names, addresses and Social Security numbers are precious assets for foreign intelligence services and terrorists who seek to fraudulently obtain travel documents needed for entry into the United States. What steps are you taking to ensure that minimum standards of privacy are in place before records that contain the private medical or financial data of American citizens – information that could provide terrorists with access to private information to support their violent objectives – are shipped off-shore?

---

[3] "Staff Statement Number 1: Entry of the 9/11 Hijackers into the United States", Seventh public hearing of the National Commission on Terrorist Attacks Upon the United States, January 26, 2004.
[4] "Pakistani Threatened UCSF To Get Paid", San Francisco Examiner, November 12, 2003.

2. What steps are you talking to prevent foreign intelligence services or terrorist elements from deriving information useful for intelligence or terrorist purposes from American medical or financial or other personally identifiable information that has been sent offshore by U.S.-based companies for processing or analysis?
3. What steps are you taking to prevent foreign intelligence services or terrorist elements from deriving information about U.S. military or intelligence personnel, U.S. government officials, U.S. law enforcement personnel or other persons in sensitive positions in the U.S. based on information transferred to offshore entities for analysis or processing?
4. As you may know, active duty, National Guard and Reserve enlisted personnel, officers and officer candidates, and their dependents are eligible for membership in the USAA family of companies, which offers its members a range of financial products and services, including brokerage services, mutual funds, financial planning, mortgage loans and insurance. According to recent news reports, USAA has outsourced part of its IT workload to Mumbai, India-based Tata Consulting Services.[5] In your view, are the physical and electronic privacy safeguards applied to USAA members' sensitive financial and medical by offshore firms such as Tata Consulting Services at least as stringent as comparable standards in the U.S.? If not, what actions do you believe are needed to ensure that the sensitive records processed or analyzed offshore receive a level of protection consistent with standards employed by U.S.-based firms? If yes, on what basis do you make this judgment?
5. In December 2002, the private records of thousands of active-duty soldiers and retired veterans were stolen from the Phoenix-based offices of TriWest Healthcare Alliance, which manages Tricare, a health care plan for the U.S. military. As a result, personal information, including names, addresses, phone numbers, Social Security numbers and medical claim histories of approximately 500,000 service members and their families were taken.[6] Although this theft occurred domestically, does your department or agency offshore the processing or analysis of its members' or dependents' health records to vendors overseas? If yes, to which offshore companies are these records exported? In which countries are these companies located? What specific measures does your department or agency take to ensure that these records receive stringent electronic and physical safeguards that are consistent with comparable standards observed in the U.S.? Has your department or agency ever terminated a contract with a vendor due to the vendor's failure to observe appropriate privacy safeguards? If yes, which vendors were involved and how many vendors were terminated since September 2001?

Thank you for your assistance in providing responses to these questions. If you have any questions about this inquiry, please feel free to have your staff contact Mr. Mark Bayer or Mr. Jeffrey S. Duncan of my staff at 202-225-2836.

Sincerely,

Edward J. Markey

Edward J. Markey
Member of Congress

[5] "More White-Collar Workers Become Casualty of Outsourcing", San Antonio Express-News, September 21, 2003.
[6] "Thieves Take Military Records", Denver Post, December 27, 2002.